STAYING SAFE

Protecting Yourself in the Virtual and Physical Worlds

STAY SAFE | REMAIN VIGILANT | PROTECT YOURSELF

March 2015, a group calling themselves the Islamic State Hacking Division posted the names and other identifying information of 100 DoD members on social media.

This appears to have been an attempt by Islamic extremists to inspire lone wolf terrorists or other radicals to commit acts of violence against the service members, utilizing the service members personal information.

FROM THE AL QAEDA HANDBOOK:

"USING PUBLIC RESOURCES OPENLY & WITHOUT RESORTING TO ILLEGAL MEANS, IT IS POSSIBLE TO GATHER AT LEAST **80%** OF INFORMATION NEEDED ABOUT THE ENEMY."

1.800.543.6289 | NCIS.NAVY.MIL | TEXT 'NCIS' + YOUR TIP INFO TO 'CRIMES' (274637) | STAYING SAFE | NCIS

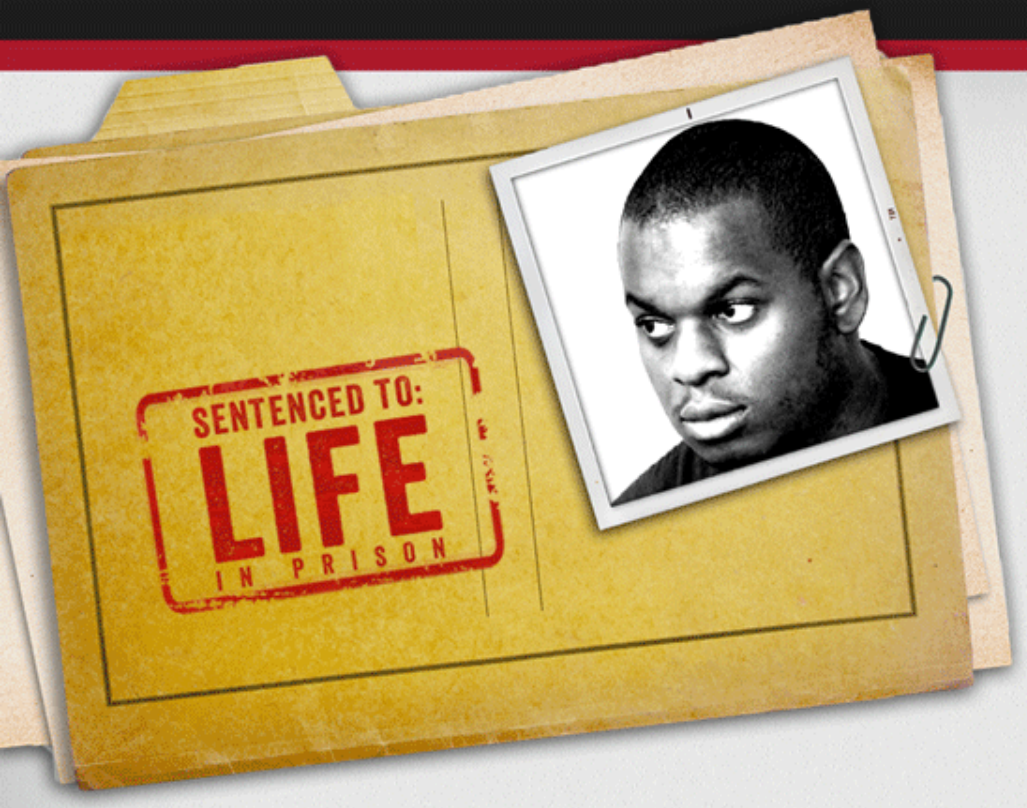
UNCLASSIFIED

WHAT MAKES YOU A TARGET?

YOUR AFFILIATION WITH THE U.S. MILITARY

What makes you stand out?

- Military uniform
- Other military identifiable items
- Posted information about U.S. military on social media or the web



CASE STUDY:
ABDULHAKIM MUJAHID MUHAMMAD

- Opened fire on Army-Navy recruiting station in Arkansas
- One recruiter killed, another wounded
- US citizen who converted to Islam in college
- Moved to Yemen in 2007 to study Islam
- Arrested in Yemen for attempting to cross into Somalia to attend bomb-making school
- Deported back to United States, interviewed by FBI and released

"I came back to America on a mission. The feds knew I had the Somali I.D. and why I had it. The reason was to go to Somalia!! To join my Mujahideen brothers and get training, because I had none. So my original plan was foiled once I was arrested in Yemen. … I had to revise another plan, and I did with the help of the Mujahideen … Al Qaeda Organization in the Arabian Peninsula"

—Abdulhakim Mujahid Muhammad

PERSONAL SECURITY

- Always be aware of your surroundings
- Don’t stand out
- Know how to contact emergency services
- Report suspicious activity

“IF YOU SEE SOMETHING,
SAY SOMETHING”

RESIDENCE SECURITY

- Identify individuals before opening doors
- Install porch light at right height
- Install dead bolts on outside doors
- Account for all house keys
- Rented residences – change locks
- Security measures with sliding glass doors and windows

1.800.543.[illegible] [illegible]NAVY.MIL TEXT 'NCIS' + YOUR TIP INFO TO 'CRIMES' (274637) STAYING SAFE NCIS
UNCLASSIFIED

VEHICLE SECURITY

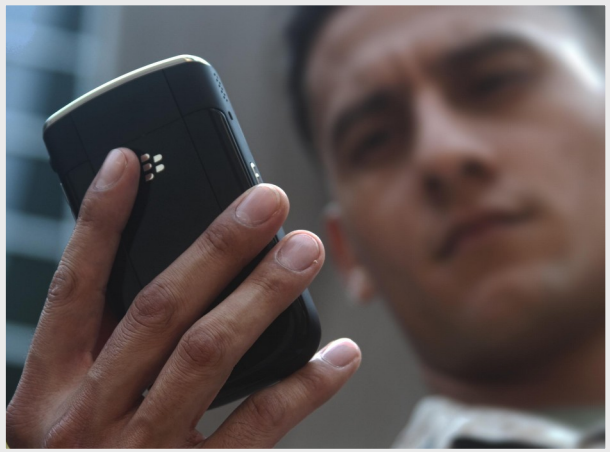
- Park in well-lit areas
- Parking Lots:
  - Where possible keep keys
  - Leave only ignition key
  - Lock car
  - Monitor attendant: Items to be put in/taken out
    only in your presence
- Home Garages:
  - Well-lit
  - Lock car doors
  - Lock garage
- Gas Tank Security
- Select a reliable service station for vehicle service

OFFICE SECURITY

- Central reception should handle visitors and packages
- Office staff should be alerted to suspicious people, parcels, and packages
- Establish key and lock controls
- Park in secured area if at all possible
- Remove names from any reserved parking areas

SOCIAL MEDIA

- Relies on connections and communication
- Encourages providing personal information
- People share more online because:
  - Sense of anonymity
  - Lack of physical interaction
  - Information shared with and for friends
  - Efforts to impress potential friends
  - False sense of security



KEEPING SAFE USING SOCIAL MEDIA SITES

- Twitter
- Facebook
- Google+ and YouTube
- Instagram
- Flickr
- Web Guide

Twitter:

If you suspect Phishing:

1) Delete any unwanted Tweets that may have been sent without your permission
2) Go to Applications > revoke access to any apps you don't recognize
3) Go to Account Settings > check phone number associated with your account, delete if not yours
4) Remind anyone with authorized access to your account to follow precautions

KEEPING SAFE USING SOCIAL MEDIA SITES

- Twitter
- Facebook
- Google+ and YouTube
- Instagram
- Flickr

Facebook:

1) Pick a unique, strong pass
2) Think before you click: never click suspicious links, even if they come from a friend or company you know.
3) Watch out for fake pages and apps/games
4) Don't accept friend requests from people you don't know.
5) Never give out your login info.

KEEPING SAFE USING SOCIAL MEDIA SITES

- Twitter
- Facebook
- Google+ and YouTube
- Instagram
- Flickr

Google+ and YouTube:
No set precaution measures but an overall reminder about security.

1) Don't use the same password on more than one site.
2) Be cautious about downloading software from the Internet
3) Be cautious about clicking on links in email messages.

KEEPING SAFE USING SOCIAL MEDIA SITES

- Twitter
- Facebook
- Google+ and YouTube
- Instagram
- Flickr

Instagram:
Same as Facebook and Twitter

If you think your account has been hacked, report it to Instagram

1) Change your password
2) Revoke access to any suspicious third-party apps

KEEPING SAFE USING SOCIAL MEDIA SITES

- Twitter
- Facebook
- Google+ and YouTube
- Instagram
- Flickr

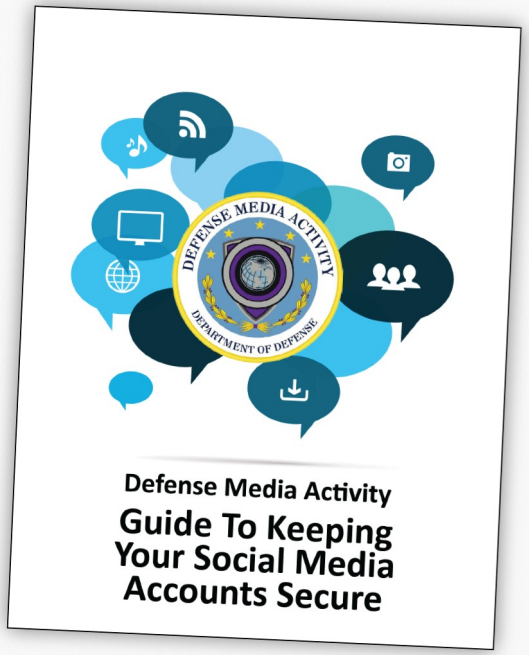
Flickr:
Photo and Video sharing community run by Yahoo

Precautions:

1) Changing your commenting controls, control who can comment on your public photos and videos
2) Change your password
3) Post with care. The community is growing and be aware of how visible the content will be.
4) Block unwanted individuals
5) Report abuse

KEEPING SAFE USING SOCIAL MEDIA SITES

- Twitter
- Facebook
- Google+ and YouTube
- Instagram
- Flickr
- Web Guide


DEFENSE MEDIA ACTIVITY
DEPARTMENT OF DEFENSE
Defense Media Activity
Guide To Keeping Your Social Media Accounts Secure

http://www.defense.gov/documents/WEB_Guide_to_Keeping_Your_Social_Media_Accounts_Secure_2015.pdf

CYBERSECURITY RISKS

- **Social Engineering**
  - Uses personal information from social media websites:
    - *Home addresses*
    - *Phone numbers*
    - *Birth dates*
    - *Family members*
    - *Hobbies*
    - *Work locations*
    - *Photos*
  - Spear Phishing
    - *Targets user*
    - *Deception to gain person information*
      - *Appears to be legitimate request*
- **Web Application Attacks**
  - Malicious content disguised as valid on social media sites

1.800.543.6289 | NCIS.NAVY.MIL | TEXT 'NCIS' + YOUR TIP INFO TO 'CRIMES' (274637) | STAYING SAFE | NCIS
UNCLASSIFIED

COMPUTER SECURITY

- Limit the personal info you post online.
- Remember what you post is public.
- Be wary of people you meet online.
- Be skeptical of links/messages asking you to update information.
- Actively manage your privacy settings.
- Protect your personal information.
- Use strong passwords and use care where you enter them.
- Vet online companies.
- Use care on unsecured wireless networks.
- Check privacy policies of sites you use regularly.
- Backup your files.
- Use automatic updates to keep all software updated, especially security software.
- Only provide personal information over encrypted websites.

1.800.543.6289 | NCIS.NAVY.MIL | TEXT 'NCIS' + YOUR TIP INFO TO 'CRIMES' (274637)
STAYING SAFE NCIS
UNCLASSIFIED

BACKGROUND CHECK WEBSITES

WHAT ARE THEY?

- Services that data mine public records, social media, business data, and other publicly available information.
- Businesses sell your data to these services for profit.

WHAT CAN YOU DO?

- Contact the service to opt out.
- Consider using a P.O. box to protect your address.
- Consider using an unlisted phone number.

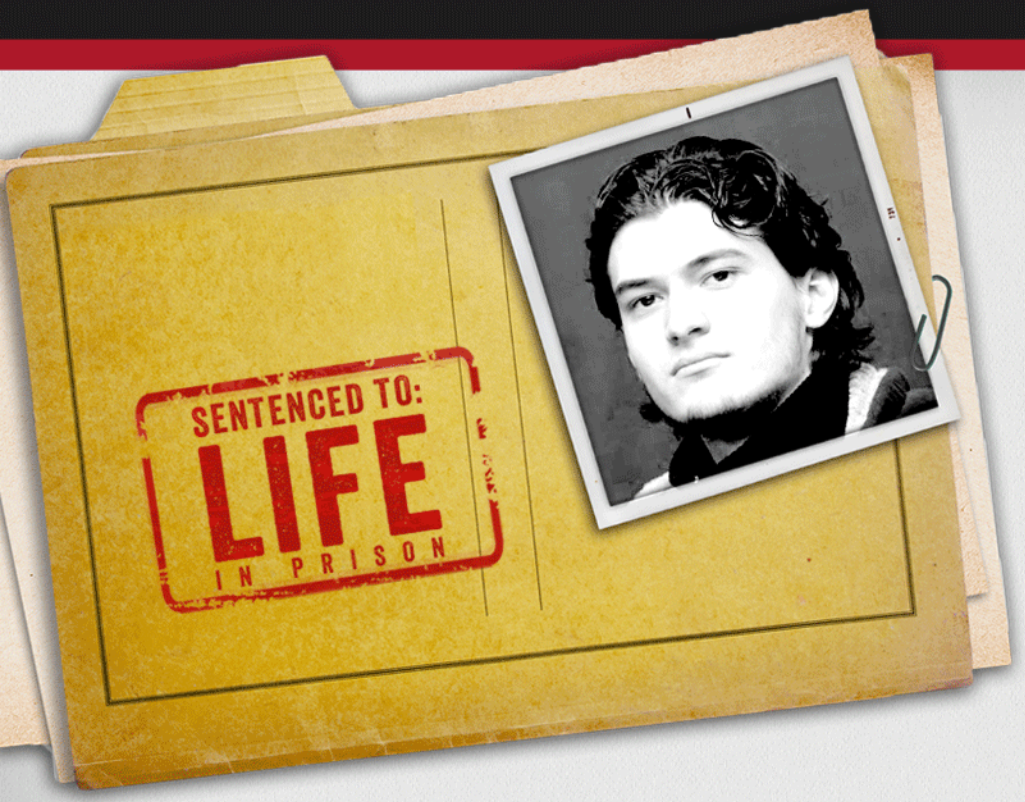
BACKGROUND CHECK WEBSITES

- Intelius.com
- Acxiom.com
- MyLife.com
- ZabaSearch.com
- Spoke.com
- BeenVerified.com
- PeekYou.com
- USSearch.com
- PeopleFinders.com
- PeopleLookup.com
- PeopleSmart.com
- PrivateEye.com
- WhitePages.com
- USA-People-Search.com
- Spokeo.com
- PublicRecordsNow.com
- DOBSearch.com
- Radaris.com

OPSEC | REMINDERS

- Think before you talk.
- Limit the information you post.
- Never speak about sensitive info in public or on unsecured lines.
- Shred sensitive information, including PII.
- Never bring home classified information.
- Create strong passwords for each account and change them often.
- Update and use security software.
- Follow the need-to-know principle.

1.800.543.6289 | NCIS.NAVY.MIL | TEXT 'NCIS' + YOUR TIP INFO TO 'CRIMES' (274637)
STAYING SAFE NCIS
UNCLASSIFIED



CASE STUDY:

ARID UKA

- Attacked U.S. Air Force bus in Frankfurt, Germany
- Killed 2 U.S. Airmen and wounded
  2 others
- Immigrated to Germany from Kosovo at a young age
- Became radicalized via the internet
- Made radical posting and friended radical imam via social media

Uka shouted "Allahu Akbar" as he committed this atrocity. He blamed the killings on the U.S. war in Afghanistan, referring to it as an invasion of Muslim lands.

WHAT TO REPORT

DoDD 5240.06 lists 10 mandated International Terrorism reportable indicators.

For an easy reference on reporting requirements, go to:

www.ncis.navy.mil *“Counterintelligence”*

REPORTABLE

INTERNATIONAL TERRORISM

CONTACTS, ACTIVITIES, INDICATORS, AND BEHAVIORS

1 2 3 4 5 6 7 8 9 10

DIRECTIVE
DoDD 5240.06

1. Advocating violence, the threat of violence, or the use of force to achieve goals on behalf of a known or suspected international terrorist organization.

2. Advocating support for a known or suspected international terrorist organizations or objectives.

3. Providing financial or other material support to a known or suspected international terrorist organization or to someone suspected of being an international terrorist.

4. Procuring supplies and equipment, to include purchasing bomb making materials or obtaining information about the

THE PROCESS OF REPORTING

REPORT FILED WITH NCIS

Reporting is simple, and methods are available 24/7:

- Local NCIS Office
- www.ncis.navy.mil
- Text "NCIS" + your tip info to CRIMES (274637)
- "Tip Submit" Android and iPhone App (select NCIS as the agency)
- 1.800.543.NAVY (6289)

Web, text, and smartphone reporting is anonymous.

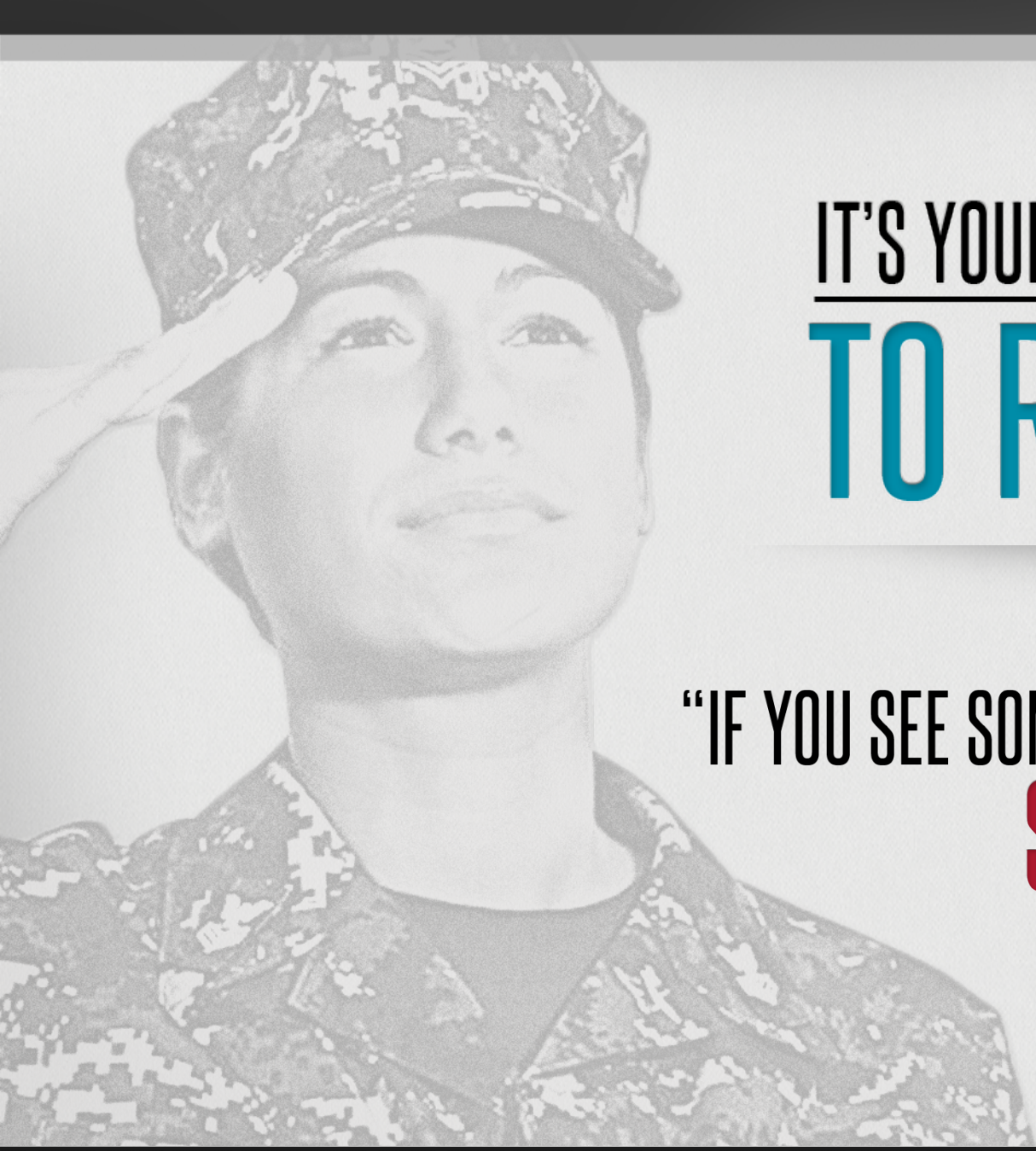
If you cannot report to NCIS, notify your security officer, supervisor, or command. Per DoDD 5240.06, they are required to notify NCIS within 72 hours.

NCIS may pay rewards up to $5,000 for information leading to a felony arrest or the prevention of certain felony crimes.

REPORTING SAVES LIVES!!!

Fort Dix Attack Thwarted

- Extremists conspired to attack personnel at Fort Dix, NJ
- Videotaped their target practice
- Brought tapes to Circuit City for transfer to DVD
- Store clerk alerted FBI
- 5 convicted of conspiracy to commit murder
- 4 received life sentences; 1 received 33 years



IT'S YOUR DUTY TO REPORT

"IF YOU SEE SOMETHING, SAY SOMETHING"